**THREATQUOTIENT** ™

**accenture**security

# THREATQ™ AND ACCENTURE SECURITY iDEFENSE®

iDefense provides clients with a comprehensive database of threat intelligence, collected over the last 20+ years, combining unique technical, operational and human intelligence sources.

With the combination of Accenture Security iDefense Threat Intelligence and the ThreatQ threat intelligence platform, organizations can empower customer environments with contextual, timely and actionable security intelligence, enabling businesses and governments to make smarter decisions to defend against new and evolving threats.

## THREATQ BY THREATQUOTIENT™

ThreatQuotient's solutions make security operations more efficient and effective. The ThreatQ open and extensible platform integrates disparate security technologies into a single security infrastructure, automating actions and workflows so that tools and people can work in unison. Empowered with continuous prioritization based on their organization's unique risk profile, security teams can focus resources on the most relevant threats, and collaboratively investigate and respond with the aim of taking the right actions faster.

## ACCENTURE SECURITY IDEFENSE THREAT INTELLIGENCE

iDefense provides clients with a comprehensive database of threat intelligence, collected over the last 20+ years, combining unique technical, operational and human intelligence sources. To help reduce the number of false positives, all iDefense threat intelligence is evaluated or vetted by our analysts. iDefense disseminates these vetted indicators for use in network security technologies to enhance their capabilities via a full-featured RESTful API for automated search and ingestion of threat intelligence content. iDefense Threat Indicators (tactical indicators of compromise) can be pushed to integration tools via the iDefense Threat Indicators Service API.
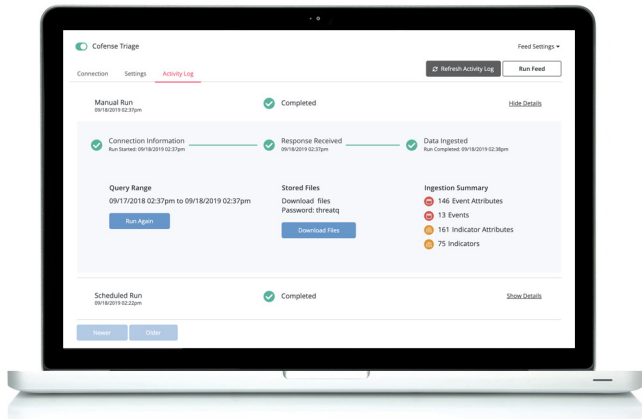
When ingesting iDefense threat intelligence into ThreatQuotient's threat intelligence platform, organizations find that they can immediately link iDefense's high-confidence and context-rich external intelligence to internal threat data and log information. Organizations are able to efficiently hunt for, look up and collect context around threats, allowing their teams to respond more efficiently and quickly to current threats.

### INTEGRATION HIGHLIGHTS

Context-Rich Intelligence: Gain context around threats, allowing teams to respond more efficiently and quickly to current threats.

Tune the ThreatQuotient Self-Tuning Threat Library™: iDefense helps tune the ThreatQuotient Self-Tuning Library with vetted indicators of compromise (IOCs) allowing teams to divert and block traffic from nefarious locations.

Provide High Confidence: iDefense provides both a "confidence" and "severity" rating for each published indicator to help prioritize indicators. This gives teams high confidence to avoid the inclusion of false positives.

## INTEGRATION USE CASES

The integration supports a variety of use cases such as:

ENHANCE PRODUCTIVITY:
Threat actors are constantly trying to penetrate your network and steal your data. SOC and IR analysts need to move just as fast, if not faster. To shorten these times, they need to quickly access relevant threat intelligence. iDefense allows you to quickly tap into a qualified resource of threat intelligence, so that you can improve your teams' productivity, accelerate work streams and create threat intelligence-fueled countermeasures.

TALENT/SKILLS SHORTAGE AUGMENTATION:
Mitigate the cyber security talent shortage and augment missing specialized threat intelligence capabilities. Ingesting iDefense intelligence allows you to augment your internal staff abilities to fill capability gaps, access knowledge from rare skill sets and quickly attain difficult threat intelligence.

ENHANCE ABILITY TO RESPOND TO THREATS:
Threat actors collaborate better without boundaries, attack faster and pivot from attack pattern to attack pattern quicker than cyber defenders can. iDefense intelligence allows you to understand how threat actors operate and move along the cyber kill chain. You can quickly arm all constituents across your organization with the right information at the right time to prioritize actions and result in a stronger team to ensure rapid defense.

## OPEN EXCHANGE ARCHITECTURE

ThreatQ's Open Exchange provides an extensible and flexible environment for analysts to achieve the optimal balance between system automation and expert analysis. Because no single security solution provides a silver bullet against attacks, ThreatQ's Open Exchange architecture supports standard interfaces for ingestion and exporting, including STIX/TAXII, XML, JSON, PDF, email and other formats of structured and unstructured data, along with an SDK and APIs for custom connections.
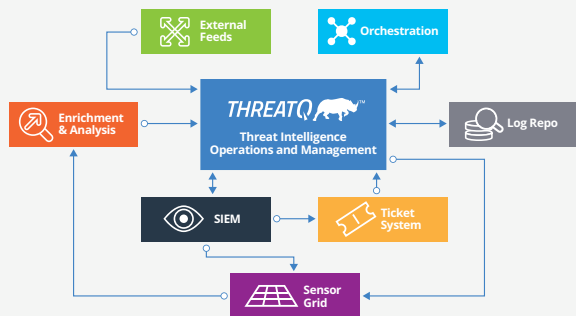


## ABOUT THREATQUOTIENT™

ThreatQuotient 's mission is to improve the efficiency and effectiveness of security operations through a threat-centric platform. By integrating an organization's existing processes and technologies into a single security architecture, ThreatQuotient accelerates and simplifies investigations and collaboration within and across teams and tools. Through automation, prioritization and visualization, ThreatQuotient's solutions reduce noise and highlight top priority threats to provide greater focus and decision support for limited resources. ThreatQuotient is headquartered in Northern Virginia with international operations based out of Europe and APAC.

For additional information, please visit threatquotient.com.

Copyright © 2019, ThreatQuotient, Inc. All Rights Reserved.

## ABOUT ACCENTURE SECURITY

Accenture Security helps organizations build resilience from the inside out, so they can confidently focus on innovation and growth. Leveraging its global network of cybersecurity labs, deep industry understanding across client value chains and services that span the security lifecycle, Accenture protects organizations' valuable assets, end-to-end. With services that include strategy and risk management, cyber defense, digital identity, application security and managed security, Accenture enables businesses around the world to defend against known sophisticated threats, and the unknown.

Follow us @AccentureSecure on Twitter or visit us at www.accenture.com/security.

TQ_ThreatQ-iDefense-Solution-Overview_Rev1

THREATQUOTIENT™  11400 Commerce Park Drive, Suite 200, Reston, VA 20191 • ThreatQuotient.com
Sales@ThreatQuotient.com • +1 703 574-9885